Chorley Council & South Ribble Borough Council

FINAL
Internal Audit Report

GDPR- Data Retention
2022/2023

Audit Assurance: Limited
Auditor: Struan Jackson
Date Issued: 15th March 2023

Cert No: 20128

WORKING TOGETHER

	Reason for the Audit & Scope
1	UK organisations that process personal information need to comply with the Data Protection Act 2018/UK General Data Protection Regulations (UK GDPR) and are required to create a data retention policy to help manage the way personal information is handled and stored. A Data Retention Policy outlines why and how data is stored, outlines how long data will be kept and how this will be disposed of, it is also fundamental to the organisations overall data management and regulatory compliance. All corporate records including emails and attachments must be managed in accordance with the Council's Data Retention Policy.
2	The review is included in the 2022/23 Audit Plan approved by the respective Governance Committee on 27th September 2022 & 23rd November 2022.

	Audit Objectives
3	The overall objective of the audit was to provide an opinion of the adequacy, application and reliability of the key internal controls put in place by management to ensure that the identified risks are being sufficiently managed.
4	The audit also assessed the effectiveness of the various other sources of assurances using the three lines of defence methodology.

	Audit Assurance
5	The Head of Internal Audit is required to provide the Governance Committee with an annual audit opinion on the effectiveness of the overall control environment operating within the Council and to facilitate this each individual audit is awarded a controls assurance rating. This is based upon the work undertaken during the review and considers the reliance we can place on the other sources of assurance.
6	Our evaluation of the reliance we can place on the three lines of defence is shown in Appendix A.
7	Both Councils have developed a suite of data management policies and operational guidance designed to ensure compliance with the requirements of GDPR, including the following documentation that aid and provide direction to officers in relation to data retention practices: • Record of Processing Activities (SRBC)/ Information Asset Registers (CBC); • Records Management Policy (SRBC)/Data Usage and Data Retention and Erasure Policy (CBC) • Data Retention Schedules; • Privacy notices. Testing identified that although both Councils have established suitably comprehensive policies and guidance there is a lack of ongoing review and monitoring to ensure that the policies and associated documentation continues to reflect the data management processes operating within the organisation. Specific weakness identified for both Councils in relation to data policies/procedures were: • Data management policies and associated guidance lack regular review and contain inaccuracies and out of date references relating to organisational structure and officer roles and responsibilities; • A number of inconsistencies were identified with the data retention periods outlined within the ROPA/Information Asset Registers, Data Retention Schedules, Privacy Notices published on Council webpages, and the actual practices identified to be operational within the Service. These practices need to be aligned to ensure a consistent approach is adopted and clear and accurate information is provided to the public. • The ROPA has not been routinely updated in line with changes in structure and responsibilities across the organisation and some data records need an updating where the responsibility for the data has changed from one Information Asset Owner (IAO) to another. Maintaining effective

records of the organisation's data processing activities is an important obligation under The Data Protection Act 2018/UK GDPR and further work is required to the Council's ROPA to ensure that it accurately reflects each organisation's current data processing environment.

- Poor accessibility to the ROPA/Information Asset Registers with a general lack of awareness amongst key officers to the location of each document.

Practices put in place to maintain focus and awareness of UK GDPR legislation appear to have waned with little evidence of cross-Council Data Management Groups operating; and routine reminders to Information Asset Owners (IAO) regarding their Record of Processing Activities (ROPA) responsibilities reducing in frequency. Completion rates for mandatory GDPR training developed to maintain staff awareness currently fall short of the 85% completion target for mandatory modules outlined within the SLT Corporate Health Dashboard (47% SRBC and 71% CBC).

Suitable guidance is available for the disposal and deletion of data at both Councils however, the majority of service areas sampled across both Council's showed poor adherence to the policy with multiple instances of storing data for a period of time exceeding that outlined in the service's ROPA/Information Asset Register/Retention Schedule/Privacy Notice; and exhibiting little awareness of the data archiving/deletion capability of the customer management system software that they were utilising. Additionally, the respective data management policies outline a specific requirement to maintain a register of destruction of records for data disposals/deletions, particularly for large scale data disposals, however, there were no examples of this being maintained for the services sampled.

Due to the number of essential improvements required to strengthen the current operational arrangements which are detailed in the action plan at Appendix B a **Limited** assurance rating has been awarded for this review. The Senior Information Risk Officer (SIRO) and the Data Protection Officer (DPO) were notified of the control weaknesses reported above during the course of our review and have committed to implement additional controls to improve management oversight and governance arrangements for compliance with GDPR these are outlined within the Management Action Plan at Appendix B.

Control Rating Key

Full – the Authority can place complete reliance on the controls. No control weaknesses exist.
Substantial - the Authority can place sufficient reliance on the controls. Only minor control weaknesses exist.
Adequate - the Authority can place only partial reliance on the controls. Some control issues need to be resolved.
Limited - the Authority cannot place sufficient reliance on the controls. Substantive control weaknesses exist

Risk and Controls	SRBC Control Evaluation	CBC Control Evaluation
Risk 1 – Lack of organisational data retention policy		
GDPR Data Management Group operational.	Action 1	Action 1
Records management policies and procedures are in place.	Action 2	Action 2
Policies/guidance is accessible for officers.	Action 3	Action 3
Officer affirmation of compliance with the Information Security Framework and associated data policies.	Action 11	Working as Intended
Officer mandatory GDPR training to support policies.	Action 4	Action 4
Risk 2 – Privacy notices are not in place or do not reflect operational arrangements		
Corporate and service specific privacy notices are in place.	Working as intended	Action 12
Privacy notices comply with the Information Commissionaire Office (ICO) requirements.	Working as intended	Working as intended
Privacy notices data retention information reflects operational requirements.	Action 5	Action 5
Risk 3 – The ROPA (Record of Processing Activity) / Information Asset Register does not accurately reflect the type of records processed.		
The ROPA / IAR's accurately records the data collected and	Action 6	Action 6

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the 'internal audit activity conforms to the Standards'

processed by the council.		
The ROPA / IAR's are reviewed and updated in compliance with GDPR requirements.	Action 6	Action 6
Council officers have access to the ROPA/Information Asset Register.	Action 7	Action 7
Regular reminders are issued to Information Asset Owners.	Action 8	Action 8
Risk 4 – Record retention schedules are not in place for each service and do not reflect practices outlined in privacy notice		
Data retention schedules are in place and regularly reviewed.	Action 2	Action 2
Data retention schedules reflect operational requirements.	Action 2	Action 2
The data retention schedules are aligned with the ROPA/ IAR's/Privacy Notices.	Action 5	Action 5
Risk 5 - Records are retained for longer than required		
Data is retained in line with operational requirements/data retention schedules.	Action 9	Action 9
Records management policies and procedures are in place.	Action 2	Action 2
Risk 6 – Procedures are in place to delete and dispose of records securely in compliance with the Data Retention Policy or service retention schedules.		
Disposal guidance is in place and available to officers.	Working as intended	Working as intended
Data disposal guidance is reviewed and updated.	Action 3	Action 3
Data is disposed of in accordance with Data management policies and other associated data related guidance material	Action 9	Action 9

*Additional risks and controls identified by Internal Audit to be added to GRACE

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the 'internal audit activity conforms to the Standards'

AUDIT ASSURANCE

Three Lines of Defence

Audit Area	1st Line	2nd Line	3rd Line	Internal Audit opinion
GDPR- Data Retention	Service Managers	Data Protection Officer	Internal Audit	Currently reliance cannot be placed on the first line of defence as the services exhibited poor adherence to the organisations data management processes and associated guidance.

Risk and Control Evaluation

Risks Examined	Full	Substantial	Adequate	Limited
Risk 1 – Lack of Organisational data retention policy				✓
Risk 2 – Privacy notices are not in place or do not reflect operational arrangements			✓	
Risk 3 – The ROPA (Record of Processing Activity) does not accurately reflect the type of records processed.				✓
Risk 4 – Record retention schedules are not in place for each service and do not reflect practices outlined in privacy notice				✓
Risk 5 - Records are retained for longer than required				✓
Risk 6 – Procedures are not in place to delete and dispose of records securely in compliance with the Data Retention Policy or service retention schedules.				✓
OVERALL AUDIT OPINION				✓

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the 'internal audit activity conforms to the Standards'

MANAGEMENT ACTION PLAN			
NO.	**FINDING**	**AGREED ACTION**	**OFFICER & DATE**
South Ribble & Chorley Findings			
1	Our review established that GDPR/Data Groups effected to support both Council's ongoing requirements of UK GDPR/Data Protection Act 2018 are no longer meeting and cannot be considered as operating. During the course of our review this weakness was acknowledged by the SIRO and DPO and commitment was provided to establish both a Data Owners Group and a Shared Information Security Council encompassing both organisations.	Agreed – The Information Security Council is to be re-established to take the strategic ownership and monitoring of performance. It will meet on a quarterly basis and will consider: the Register of Processing Activity; receive reports from Data Owners Group changes to policies retention periods new data use receive reports of ICO reporting.	Director of Governance June 23
2	Testing identified that both Councils have comprehensive policies in place that provide guidance to officers on the management, use, retention and deletion of data, however, testing identified a lack of regular review resulting in inaccuracies/errors with organisational structure/roles and responsibilities, and incomplete data retention schedules that do not reflect the current needs each service and the organisation as a whole.	A new suite of policies has been drafted and will be presented to SMT for review / approval. New policies include: Data Breach policy; Data Protection policy; Data Retention and Erasure policy; Data Usage policy; Information classification policy; Subject access request policy. Once agreed with SMT, policies will be shared and awareness raised.	Director of Customer and Digital June 23
3	Data management policies and other associated data related	Agreed – awareness will be raised via SLT / core briefs and a	Director Customer

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the 'internal audit activity conforms to the Standards'

	guidance material can be found on both Council's intranets however, these were not easy to locate, do not align, and contain links to empty folders/missing information. Furthermore, testing identified that many key officers were uncertain where to locate this documentation. To ensure that accurate, relevant and up to date information is available to officers to support the data management policies, processes and legal requirements the guidance on both Council's intranets should be assessed and updated as soon as possible; and given suitable prominence on the Council's intranet.	dedicated page on the intranets will be established.	and Digital June 23
4	Testing established that the completion rates for the GDPR mandatory module within Learning Hub falls short of the 85% completion target for mandatory modules outlined within the SLT Corporate Health Dashboard (47% SRBC and 71% CBC). Further work is required to ensure that all Council staff complete the mandatory training. During the course of our review this weakness was acknowledged by the SIRO and DPO and commitment was provided to review data management training requirements.	Agreed by SMT. Each member of SMT to ensure that mandatory training is completed by all Council staff.	Senior Management Team September 2023
5	Privacy notices are available to the public on both Councils websites and our review confirmed that the format of privacy notices sampled complied with the Information Commissionaire Office (ICO) requirements. However, further comparison of the sampled privacy notices against corporate data retention schedules found that the information provided was not aligned for a number of services reviewed.	Agreed by SMT Each member of SMT will ensure that privacy notices are reviewed and updated to reflect the current data retention schedules.	Senior Management Team September 2023

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the 'internal audit activity conforms to the Standards'

	There is a need for services to ensure that the information on the data retention schedules is accurate and that this information matches that provided to customers within the published privacy notice to ensure that the Council is being clear and transparent with how it is handling personal and sensitive data.		
6	Testing identified that both Councils have a Record of Processing Activities (ROPA/Information Asset Register) that provides an overview of the organisations data processing activities however, a review of these documents identified that they are not fully completed and are not being revisited and updated on a regular basis in line with corporate guidance. Both Council's need to ensure that the ROPA is suitably comprehensive covering all services areas/functions; and that they have effective processes in place to keep the ROPA record up to date. A poorly maintained ROPA may put the Council at risk of not meeting its obligations under the DPA 2018/UK GDPR.	Agreed by SMT. Each member of SMT will ensure that the ROPA / Information Asset Registers are updated and accurately reflect current operational activity. The Information Security Council will ensure that going forwards ROPAs / Information Asset Registers are maintained.	Senior Management Team September 2023
7	Our review identified issues at both Councils with the prominence and accessibility of the ROPA/Information Asset Register/s. During the course of our review the document was either not readily available on the intranet (SRBC), or it was located on a page that was hard to locate/poorly labelled (CBC). It was acknowledged during the course of our review that access to the ROPA was reinstated for SRBC, however further consideration should be given to the prominence/location of this document at both Council's so that the ROPA can be easily accessed and readily available to officers (IAOs) tasked with adding, removing and amending the information contained within.	Agreed – awareness will be raised via SLT / core briefs and a dedicated page on the intranets will be established	Director Customer and Digital June 23

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the 'internal audit activity conforms to the Standards'

8	Evidence was available to show that an email reminder has been issued by the Data Protection Officer within the last 12 months to maintain IAO awareness of the ROPA/Information Asset Register and their associated data management responsibilities however, the frequency of reminders has decreased since this was last reviewed by Internal Audit in March 2022.	Agreed – this will form part of the monitoring undertaken by the Information Security Council and reminders / updates will be requested on a quarterly basis.	Director of Governance June 23
9	It is a requirement of both Council's data management policies that "personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed". The review highlighted a number of service areas across both Council's failing to follow the data retention/deletion requirements of the data management policies holding data in excess of business need and/or for a period of time exceeding that outlined in the ROPA/Information Asset Register/Retention Schedule/Privacy Notice. Furthermore, services sampled also exhibited little awareness of the data archiving/deletion capability of the customer management system software that they were utilising to process personal data.	Agreed by SMT Each member of SMT will ensure that their Directorates review data held (both paper based and electronically) to ensure compliance with their data retention schedules.	Senior Management Team September 2023
10	A specific requirement of the respective data management policies for each Council is to maintain a register of destruction of records for data disposals/deletions. Where our testing did identify examples of good data management and expired data had been deleted in accordance with the agreed arrangements, a register of disposal had not been maintained.	Agreed by SMT Each member of SMT will ensure that a register of destruction of records for data disposals is completed and maintained going forwards.	Senior Management Team September 2023

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the 'internal audit activity conforms to the Standards'

South Ribble Only Findings			
11	Prior to logging into the Council's joint network each day officers are required to affirm that they understand and agree to the requirements of the Information Security Framework and its associated data policies including the Corporate Data Usage Policy (CDUP). Testing identified that the CDUP is not available to South Ribble officers on Connect or via the Learning Hub and appears to be a CBC only policy, not applicable to South Ribble officers.	Shared policies being developed and awareness to be raised.	Complete
Chorley Only Findings			
12	Testing identified that Legal Services did not have a privacy notice in place and available to view on the Council's website. To comply with the requirements of GDPR, privacy notices are required where personal data is processed.	Agreed – Privacy notice will be placed on the website	Director of Governance June 23
	Outside the agreed scope for this review, testing identified that there is the opportunity to align processes and policies given the expansion of shared services between Chorley Council and South Ribble Council and the similarity of the Council's data processing requirements. This option should be explored further when considering actions for the above findings. During the course of our review this weakness was acknowledged by the SIRO and DPO and commitment was provided to align and re-publish data management policies across both Councils.	See action 2	

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the 'internal audit activity conforms to the Standards'

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the ‘internal audit activity conforms to the Standards’